# Least Common Mechanism

Sean Barnum, Cigital, Inc. [vita[3]]
Michael Gegick, Cigital, Inc. [vita[4]]

2005-09-14

Avoid having multiple subjects sharing mechanisms to grant access to a resource. For example, serving an application on the Internet allows both attackers and users to gain access to the application. Sensitive information can potentially be shared between the subjects via the mechanism. A different mechanism (or instantiation of a mechanism) for each subject or class of subjects can provide flexibility of access control among various users and prevent potential security violations that would otherwise occur if only one mechanism was implemented.

## Detailed Description Excerpts

According to Saltzer and Schroeder [Saltzer 75] in "Basic Principles of Information Protection" from pages 9-10:

> Least common mechanism: Minimize the amount of mechanism common to more than one user and depended on by all users.[8] Every shared mechanism (especially one involving shared variables) represents a potential information path between users and must be designed with great care to be sure it does not unintentionally compromise security. Further, any mechanism serving all users must be certified to the satisfaction of every user, a job presumably harder than satisfying only one or a few users. For example, given the choice of implementing a new function as a supervisor procedure shared by all users or as a library procedure that can be handled as though it were the user's own, choose the latter course. Then, if one or a few users are not satisfied with the level of certification of the function, they can provide a substitute or not use it at all. Either way, they can avoid being harmed by a mistake in it.

According to Bishop [Bishop 03] in Chapter 13, "Design Principles," in 13.2.7, "Principle of Least Common Mechanism," from page 348:[9]

> This principle is restrictive because it limits sharing.

> Definition 13-7. The principle of least common mechanism states that mechanisms used to access resources should not be shared.

> Sharing resources provides a channel along which information can be transmitted, and so such sharing should be minimized. In practice, if the operating system provides support for virtual machines, the operating system will enforce this privilege automatically. Otherwise, it will provide some support (such as a virtual memory space) but not complete support (because the file system will appear as shared among several processes).

---

3.   daisy:35 (Barnum, Sean)

4.   daisy:345 (Gegick, Michael)

8.   G. Popek, "A principle of kernel design," *in 1974 NCC, AFIPS Cong. Proc.*, vol. 43, pp.977-978. (I-A3).

9.   All rights reserved. It is reprinted with permission from Addison-Wesley Professional.

**Example 1**

A web site provides electronic commerce services for a major company. Attackers want to deprive the company of the revenue they obtain from that web site. They flood the site with messages, and tie up the electronic commerce services. Legitimate customers are unable to access the web site and, as a result, take their business elsewhere.

Here, the sharing of the Internet with the attackers' sites caused the attack to succeed. The appropriate countermeasure would be to restrict the attackers? access to the segment of the Internet connected to the web site. Techniques to do this include proxy servers such as the Purdue SYN intermediary[10] or traffic throttling. The former targets suspect connections; the latter reduces load on the relevant segment of the network indiscriminately.

## References

[Bishop 03]        Bishop, Matt. *Computer Security: Art and Science*. Boston, MA: Addison-Wesley, 2003.

[Saltzer 75]       Saltzer, Jerome H. & Schroeder, Michael D. "The Protection of Information in Computer Systems," 1278-1308. *Proceedings of the IEEE 63,* 9. IEEE, September 1975.

# Cigital, Inc. Copyright

# Pola

| Nazwa | Warto## |
|---|---|
| Copyright Holder | Cigital, Inc. |

# Pola

---

10.  C. Schuba, I. Krsul, M. Kuhn, E. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a Denial of Service Attack on TCP," *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, pp. 208-223 (May 1997).

1.  mailto:copyright@cigital.com

---

| Nazwa | Warto## |
|---|---|
| is-content-area-overview | false |
| Content Areas | Knowledge/Principles |
| SDLC Relevance | Design |
| Workflow State | Publishable |